



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

7590 03/07/2005

David B Cochran  
Jones Day Reavis & Pogue  
North Point  
901 Lakeside Avenue  
Cleveland, OH 44114

EXAMINER

TESLOVICH, TAMARA

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/594,368

Applicant(s)

LITTLE, HERB A.

Examiner

Tamara Teslovich

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 27 December 2004.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-45 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-45 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/27/04</u> . | 6) <input type="checkbox"/> Other: _____  |

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-10, 16-25, and 31-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Vanstone et al., US Pat 5,761,305. Alfred Menezes, Paul van Oorschot and Scott Vanstone's *Handbook of Applied Cryptography*, hereinafter referred to as *Applied Cryptography*, has been relied upon for inherent qualities of public-key cryptosystems.

Regarding Claims 1, 16, and 31, Vanstone teaches a public-key encryption process and system comprising the steps of:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair (see Vanstone col.3 lines 1-7, 39-43); and

b) signing a digital signature using the ephemeral key pair (see Vanstone col.3 lines 1-10; col.4 lines 62-64; see also *Applied Cryptography* section 12.5.2, Remark 12.41).

Please note that although the phrase 'ephemeral key pair' does not appear in the Vanstone reference, Vanstone's key pair is generated new each time it is needed, without repetition and discarded once used, which by definition makes it an ephemeral key pair.

Regarding Claims 2, 17, and 32, Vanstone teaches a public-key encryption process and system wherein the encrypting step uses an El Gamal encryption scheme (see Vanstone col.3 line 60 thru col.4 line 40; see also Applied Cryptography section 12.5.2).

Regarding Claim 3, Vanstone teaches a public-key encryption process wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme;

wherein the step of generating the digital signature includes hashing the plaintext message (col.3 line 60 thru col.4 line 40; see also Applied Cryptography sections 9.1 and 12.5.2). (Note that reference to 'ElGamal-family signature schemes' includes the Nyberg-Rueppel digital signature scheme).

Regarding Claims 18, and 33, Vanstone teaches a public-key encryption process and system wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme (see Vanstone col.3 line 60 thru col.4 line 40; see also Applied Cryptography sections 9.1 and 12.5.2). (Note

Art Unit: 2137

that reference to 'ElGamal-family signature schemes' includes the Nyberg-Rueppel digital signature scheme).

Regarding Claims 4, 19, and 34, Vanstone teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key  $x$  and calculating an encryption ephemeral public key  $X = xG$ , where  $G$  is a generator (see Vanstone col.3 lines 1-5; see also Applied Cryptography section 8.4 and Algorithm 8.17).

Regarding Claims 5, 20, and 35, Vanstone teaches a public-key encryption process and system for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key  $a$ ; and

b) calculating a sender public key  $A = aG$ , where  $G$  is a generator,

and at the receiver,

a) generating a receiver private key  $b$ ; and

b) calculating a receiver public key  $B = bG$ ,

wherein the sender obtains an authentic copy of the receiver public key  $B$  and the receiver obtains an authentic copy of the sender public key  $A$  (see Vanstone col.3 line 60 thru col.4 line 4; see also Applied Cryptography section 8.4.1).

Art Unit: 2137

Regarding Claims 6, 21, and 36, Vanstone teaches a public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key  $x$  and calculating an encryption ephemeral public key  $X = xG$  (see Vanstone col.3 lines 5-7; see also Applied Cryptography sections 8.4.1, 12.2.2, 12.5.2, and Remark 12.41).

Regarding Claims 7, 22, and 37, Vanstone teaches a public-key encryption process and system, further comprising the steps of,

at the sender,

generating a secret key  $K = xB$  and encrypting a plaintext message using the secret key  $K$  to generate a ciphertext message (see Vanstone col.3 lines 21-24, 39-43; see also Applied Cryptography section 8.4.1).

Regarding Claims 8, 23, and 38, Vanstone teaches a public-key encryption process and system, further comprising the steps of,

at the sender,

using the encryption private key  $x$  as a signature ephemeral private key and using the encryption ephemeral public key  $X$  as a signature ephemeral public key to generate a digital signature (see Vanstone col.3 lines 5-7; see also Applied Cryptography sections 11.5.4, 12.2.2, 12.5.2, and Remark 12.41).

Regarding Claims 9, 24 and 39, Vanstone teaches a public-key encryption process and system,

wherein the digital signature comprises a first value  $r$  and a second value  $s$ , the process further comprising the step of,

at the sender,

transmitting the encryption ephemeral public key  $X$ , the ciphertext message and the second value  $s$  of the digital signature to the receiver (see Vanstone col.3 lines 8-10; col.4 lines 27-29; see also Applied Cryptography section 11.5.4).

Regarding Claims 10, 25, and 40, Vanstone teaches a public-key encryption process and system, further comprising the steps of,

at the receiver,

generating the secret key  $K = bX = bxG = xbG = xB$ ,

decrypting the transmitted ciphertext message using the generated secret key  $K$ ,

calculating the first value  $r$  of the digital signature using the decrypted message and the transmitted encryption ephemeral public key  $X$  and

validating the digital signature based on the calculated first value  $r$  and the transmitted second value  $s$  (see Vanstone col.3 lines 21-29, 47-51; see also Applied Cryptography section 11.5.4).

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 11-15, 26-30, and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone and Applied Cryptography as applied to claim 1-10, 16-25 and 31-40 above, and further in view of Boyd et al.'s "Key Establishment Protocols for Secure Mobile Communications".

Regarding Claim 11, Vanstone teaches a the public-key encryption process of Claim 1, wherein at least a two-stage public-key encryption process is used; wherein the first stage includes key establishment and the second stage includes encryption/decryption (see Vanstone col.3 lines 52-59); wherein said steps (a) and (b) are performed during the second stage of encryption (see Vanstone col.3 lines 44-51).

Vanstone does not teach the abovementioned encryption process implemented in a wireless communication system or device.

Boyd et al. teaches the implementation of a public-key encryption process and system in a wireless communication system (see Boyd).



It would be obvious to one of ordinary skill in the art to employ the public key encryption process and system of Vanstone within a wireless communication system to secure information being transmitted wirelessly.

Regarding Claims 12-15, 26-30 and 41-45, Vanstone teaches a public-key encryption process and system, but fails to teach its implementation in a wireless hand-help communication system.

Boyd et al. teaches the implementation of a public-key encryption process and system in a wireless communication system (see Boyd).

It would be obvious to one of ordinary skill in the art to employ the public key encryption process and system of Vanstone within a wireless communication system or device to secure information being transmitted wirelessly.

Claims 1, 16, and 31 are also rejected under 35 U.S.C. 102(b) as being anticipated by the IBM System Digital Signature Data Structure Format, IBM TDB NN9305343.

Regarding Claims 1, 16, and 31, IBM teaches a public-key encryption process and system comprising the steps of:

- a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair (see IBM); and
- b) signing a digital signature using the ephemeral key pair (see IBM).

Although Examiner finds the entire IBM document relevant, attention is drawn to the following passage:

"The cryptographic facility access program (CFAP) contains cryptographic algorithms consisting of the DEA and RSA public key algorithm, each capable of performing encrypt and decrypt operations. The CFAP contains a function to generate a pair of RSA keys, which is called PKG. The CFAP contains a set of cryptographic functions, which, as a by-product of function execution, generate a system digital signature. The CFAP also contains an Application Signature Generate (ASG) function for producing application digital signatures."

Note that although the phrase 'ephemeral key pair' does not appear in the abovementioned passage, IBM utilizes the RSA algorithm, which is known to utilize session keys, which are by definition ephemeral keys. For example, SSL has been using these ephemeral RSA keys publicly as far back as 1993.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone

Art Unit: 2137

number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Tamara Teslovich  
March 1, 2005



ANDREW CALDWELL  
SUPERVISORY PATENT EXAMINER